

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-306088

(43)Date of publication of application : 05.11.1999

(51)Int.Cl.

G06F 12/14
G06K 17/00
G06K 19/073
G09C 1/00
H04L 9/32

(21)Application number : 10-117394

(71)Applicant : TOPPAN PRINTING CO LTD

(22)Date of filing : 27.04.1998

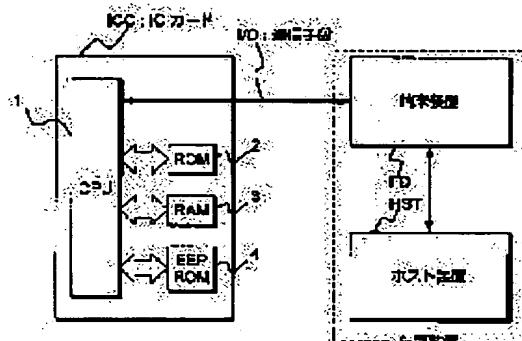
(72)Inventor : YURA AKIYUKI
MATSUMURA SHUICHI
FUNADOGAWA NORIO

(54) IC CARD AND IC CARD SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an IC card and IC card system capable of preventing IC card data from being illegally obtained.

SOLUTION: A CPU 1 unidirectionally adds or subtracts a specified value to/from additional data stored in an EEPROM 4 each time a piece of instruction data is received from a terminal device IFD. Moreover, the CPU 1 adds the added or subtracted additional data to the instruction data, allows a specific secret key to encipher the instruction data with these addition data added, and makes them data which are transmitted and received on a communication means.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 1 - 3 0 6 0 8 8

(43) 公開日 平成 1 1 年 (1 9 9 9) 1 1 月 5 日

(51) Int. Cl.	識別記号	庁内整理番号	F I	技術表示箇所
G06F 12/14	320		G06F 12/14	320 A
G06K 17/00			G06K 17/00	E
19/073			G09C 1/00	660 A
G09C 1/00	660		G06K 19/00	P
H04L 9/32			H04L 9/00	675 A
審査請求 未請求 請求項の数 1 0 O L (全 8 頁)				

(21) 出願番号 特願平 1 0 - 1 1 7 3 9 4

(22) 出願日 平成 1 0 年 (1 9 9 8) 4 月 2 7 日

(71) 出願人 0 0 0 0 0 3 1 9 3

凸版印刷株式会社

東京都台東区台東 1 丁目 5 番 1 号

(72) 発明者 由良 彰之

東京都台東区台東 1 丁目 5 番 1 号 凸版印刷株式会社内

(72) 発明者 松村 秀一

東京都台東区台東 1 丁目 5 番 1 号 凸版印刷株式会社内

(72) 発明者 船渡川 紀夫

東京都台東区台東 1 丁目 5 番 1 号 凸版印刷株式会社内

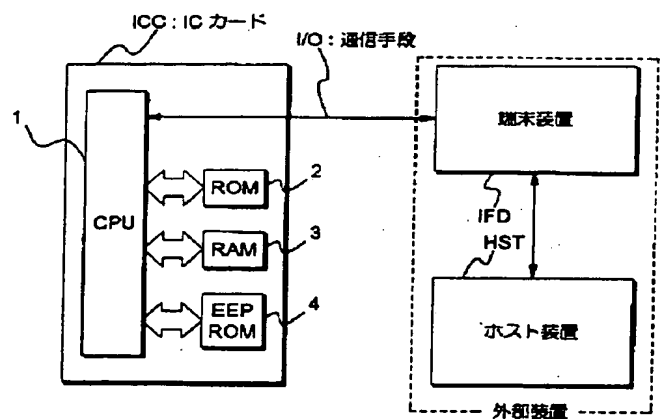
(74) 代理人 弁理士 川▲崎▼ 研二

(54) 【発明の名称】 I C カードおよび I C カードシステム

(57) 【要約】

【課題】 不正に I C カードのデータを入手することを防止する I C カードおよび I C カードシステムを提供する。

【解決手段】 CPU 1 は、EEPROM 4 に格納されるデータである付加データに対して、一つの命令データを端末装置 I F D 側から受信する毎に所定値を一方向的に加算又は減算する。さらに、CPU 1 は、その加算又は減算された付加データを前記命令データに付加し、この付加データが付加された命令データを特定の秘密鍵によって暗号化して通信手段上で送受信されるデータとする。



【特許請求の範囲】

【請求項 1】 外部装置から受信した命令データに従って所定の処理を行う IC カードにおいて、

前記命令データを認証するための認証データを記憶する認証データ記憶手段と、

前記認証データを、前記受信に先だって前記外部装置に送信する認証データ送信手段と、

前記認証データと前記命令データとに基づいて生成された認証付命令データを受信すると、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較し、当該比較結果に基づいて、前記命令データが正当なデータであるか否かを判定する判定手段とを具備することを特徴とする IC カード。

【請求項 2】 前記認証付命令データは、前記認証データを付加した前記命令データを暗号化して生成されており、

前記判定手段は、前記認証付命令データを復号化することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする請求項 1 に記載の IC カード。

【請求項 3】 前記認証付命令データは、前記認証データを付加した前記命令データを暗号化した暗号化認証データと前記命令データとを含んで生成されており、

前記判定手段は、前記認証データ記憶手段に記憶された認証データを付加した前記認証付命令データ中の前記前記命令データを暗号化して比較データを生成し、当該比較データと前記暗号化認証データとを比較することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする請求項 1 に記載の IC カード。

【請求項 4】 当該外部装置から前記認証付命令データを受信する毎に、前記認証データ記憶手段に記憶された認証データを更新する認証制御手段をさらに具備することを特徴とする請求項 1 ないし 3 いずれかに記載の IC カード。

【請求項 5】 前記判定手段は、前記認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとの差が所定の範囲内であれば、前記命令データが正当なデータであると判定し、

前記認証制御手段は、前記認証データに所定の演算を行うことによって前記更新を行うことを特徴とする請求項 4 に記載の IC カード。

【請求項 6】 外部装置と、当該外部装置から受信した命令データに従って所定の処理を行う IC カードとを具備する IC カードシステムにおいて、

前記 IC カードは前記命令データを認証するための認証データを記憶する認証データ記憶手段と、

前記認証データを、前記受信に先だって前記外部装置に送信する認証データ送信手段とを具備し、

前記外部装置は、

受信した前記認証データと前記命令データとに基づいて認証付命令データを生成する認証付命令データを生成手段と、

前記認証付命令データを前記 IC カードに送信する認証付命令データ送信手段を具備し、

前記 IC カードは、

前記認証付命令データを受信すると、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較し、当該比較結果に基づいて、

前記命令データが正当なデータであるか否かを判定する判定手段とを具備することを特徴とする IC カードシステム。

【請求項 7】 前記認証付命令データ生成手段は、前記認証データを付加した前記命令データを暗号化して前記認証付命令データを生成し、

前記判定手段は、前記認証付命令データを復号化することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする請求項 6 に記載の IC カードシステム。

【請求項 8】 前記認証付命令データ生成手段は、前記認証データを付加した前記命令データを暗号化した暗号化認証データと前記命令データとを含んだ前記認証付命令データを生成し、

前記判定手段は、前記認証データ記憶手段に記憶された認証データを付加した前記認証付命令データ中の前記前記命令データを暗号化して比較データを生成し、当該比較データと前記暗号化認証データとを比較することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする請求項 6 に記載の IC カードシステム。

【請求項 9】 当該外部装置から前記認証付命令データを受信する毎に、前記認証データ記憶手段に記憶された認証データを更新する認証制御手段をさらに具備することを特徴とする請求項 6 ないし 8 いずれかに記載の IC カードシステム。

【請求項 10】 前記判定手段は、前記認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとの差が所定の範囲内であれば、前記命令データが正当なデータであると判定し、

前記認証制御手段は、前記認証データに所定の演算を行うことによって前記更新を行うことを特徴とする請求項 9 に記載の IC カードシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、データを利用者が物理的に持ち運びできるシステムである IC カードに代表される可搬型データ担拠システムに係り、特に、不正にデータが入手されることを防止するのに好適な IC

カードおよび IC カードシステムに関する。

【 0 0 0 2 】

【従来の技術】従来の IC カードは、IC カードに内蔵されている記憶手段に格納されているデータへの読み書きを、各ファイル毎に複数のパスワードを組み合わせたアクセス権を用いて管理し、データのセキュリティを保っている。なお、通常、IC カードでは、記憶手段内にデータを格納する場合にファイルという概念を適用している。

【 0 0 0 3 】また、前述のアクセス権とは、ファイル毎に設定されているものであり、通常、データの読み出しに関するアクセス権、データの書き換えに関するアクセス権等、ファイルに対する命令の種類毎に複数種類設定できるものである。IC カード内には、そのアクセス権の種類に対応する数のパスワードデータが格納されており、アクセス権の許可は、各ファイル毎に規定されたアクセス権に対応したパスワードを照合することで行っている。つまり正当な権原者とは、IC カード内に格納されたパスワードデータを知り得る者である。

【 0 0 0 4 】例えば、正当権原者によるデータの読み出しには、図 2 に示すフローチャートのように、まず、当該ファイルに設定されている読み出し命令に対応するアクセス権を満足させるために、パスワード照合コマンドにパスワードデータである秘密鍵データを付加して IC カードに送信する (S 1 1) 。そして、IC カードはその受信した秘密鍵データが IC カード内に格納されているものと同一か否かを比較照合する (S 1 2) 。

【 0 0 0 5 】ここで、受信した秘密鍵データが IC カード内に格納されているものと同一であれば、アクセス権を当該読み出し命令に与えるべく、当該秘密鍵の照合状態を照合済みに設定し (S 1 3) 、照合が成功した旨を返答データとして端末側に送信する (S 1 4) 。その後、送信されてくる正当な当該ファイルに対するデータ読み出し命令に対し (S 1 5) 、指定されたアロケーションのデータを返信データとして送信する (S 1 6) 。

【 0 0 0 6 】一方、ステップ 1 2 において、受信した秘密鍵データが IC カード内に格納されているものと同一でない場合は、当該秘密鍵の照合状態を未照合に変更し (S 1 7) 、変数である連続間違え回数に 1 を加算する (S 1 8) 。そして、その加算した連続間違え回数と事前に規定している連続間違え許容回数とを照らし合わせ (S 1 9 、 S 2 0) 、当該連続間違え回数が連続間違え許容回数と一致した場合、若しくは当該連続間違え回数が連続間違え許容回数よりも大きくなった場合は、当該秘密鍵データが格納されているファイルを閉鎖状態とする (S 2 1) 。そして、照合が失敗した旨を返答データとして端末側に送信する (S 2 2) 。

【 0 0 0 7 】

【発明が解決しようとする課題】ところで、正当権利者が前述の図 2 に示す手順にしたがってパスワードの照合

を終了し、当該ファイルに対する読み出し権を獲得した後、不正アクセス者が IC カードの通信手段に侵入して、正当アクセス者が送信したデータを不正アクセス者が複製等することで正当な読み出し命令を IC カードに対し送信した場合は、当該 IC カードは不正アクセス者に対して前記返信データを返信してしまうという事態が考えられる。このことは、現状の IC カードでは防ぎようのないセキュリティ上の抜け道であった。

【 0 0 0 8 】本発明に係る事情に鑑みてなされたものであり、正当アクセス者が送信したデータを不正アクセス者が複製して送信することで、不正に IC カードのデータを入手することを防止する IC カードおよび IC カードシステムを提供することを目的とする。

【 0 0 0 9 】

【課題を解決するための手段】上述した課題を解決するために請求項 1 記載の発明は、外部装置から受信した命令データに従って所定の処理を行う IC カードにおいて、前記命令データを認証するための認証データを記憶する認証データ記憶手段と、前記認証データを、前記受信に先だって前記外部装置に送信する認証データ送信手段と、前記認証データと前記命令データとに基づいて生成された認証付命令データを受信すると、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較し、当該比較結果に基づいて、前記命令データが正当なデータであるか否かを判定する判定手段とを具備することを特徴とする。

【 0 0 1 0 】また、請求項 2 に記載の発明は、請求項 1 に記載の発明において、前記認証付命令データは、前記認証データを付加した前記命令データを暗号化して生成されており、前記判定手段は、前記認証付命令データを復号化することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする。

【 0 0 1 1 】また、請求項 3 に記載の発明は、請求項 1 に記載の発明において、前記認証付命令データは、前記認証データを付加した前記命令データを暗号化した暗号化認証データと前記命令データとを含んで生成されており、前記判定手段は、前記認証データ記憶手段に記憶された認証データを付加した前記認証付命令データ中の前記前記命令データを暗号化して比較データを生成し、当該比較データと前記暗号化認証データとを比較することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする。

【 0 0 1 2 】また、請求項 4 に記載の発明は、請求項 1 にないし 3 いずれかに記載の発明において、当該外部装置から前記認証付命令データを受信する毎に、前記認証データ記憶手段に記憶された認証データを更新する認証制御手段をさらに具備することを特徴とする。

【 0 0 1 3 】また、請求項 5 に記載の発明は、請求項 4

に記載の発明において、前記判定手段は、前記認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとの差が所定の範囲内であれば、前記命令データが正当なデータであると判定し、前記認証制御手段は、前記認証データに所定の演算を行うことによって前記更新を行うことを特徴とする。

【0014】また、請求項6に記載の発明は、外部装置と、当該外部装置から受信した命令データに従って所定の処理を行うICカードとを具備するICカードシステムにおいて、前記ICカードは前記命令データを認証するための認証データを記憶する認証データ記憶手段と、前記認証データを、前記受信に先だって前記外部装置に送信する認証データ送信手段とを具備し、前記外部装置は、受信した前記認証データと前記命令データとに基づいて認証付命令データを生成する認証付命令データ生成手段と、前記認証付命令データを前記ICカードに送信する認証付命令データ送信手段を具備し、前記ICカードは、前記認証付命令データを受信すると、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較し、当該比較結果に基づいて、前記命令データが正当なデータであるか否かを判定する判定手段とを具備することを特徴とする。

【0015】また、請求項7に記載の発明は、請求項6に記載の発明において、前記認証付命令データ生成手段は、前記認証データを付加した前記命令データを暗号化して前記認証付命令データを生成し、前記判定手段は、前記認証付命令データを復号化することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする。

【0016】また、請求項8に記載の発明は、請求項6に記載の発明において、前記認証付命令データ生成手段は、前記認証データを付加した前記命令データを暗号化した暗号化認証データと前記命令データとを含んだ前記認証付命令データを生成し、前記判定手段は、前記認証データ記憶手段に記憶された認証データを付加した前記認証付命令データ中の前記前記命令データを暗号化して比較データを生成し、当該比較データと前記暗号化認証データとを比較することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする。

【0017】また、請求項9に記載の発明は、請求項6ないし8いずれかに記載の発明において、当該外部装置から前記認証付命令データを受信する毎に、前記認証データ記憶手段に記憶された認証データを更新する認証制御手段をさらに具備することを特徴とする。

【0018】また、請求項10に記載の発明は、請求項9に記載の発明において、前記判定手段は、前記認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとの差が所定の範囲内であ

ば、前記命令データが正当なデータであると判定し、前記認証制御手段は、前記認証データに所定の演算を行うことによって前記更新を行うことを特徴とする。

【0019】

【発明の実施の形態】以下、図面を参照して、この発明の実施形態を説明する。

A：実施形態の構成

【0020】図1は、本発明の1の実施形態であるICカードシステムの構成を示すブロック図である。図示するように、本発明にかかるICカードICCは、外部装置と通信手段I/Oを介して通信可能に接続でき、外部装置は、ICカードICCに対してアクセスを行うための装置である端末装置IFDと、端末装置IFDと接続されたホスト装置HSTとを備えている。

【0021】ICカードICCは、CPU1、ROM2、RAM3、およびEEPROM4を備えている。CPU1は、ROM2に格納されている当該ICカードのオペレーティングシステムであるカードOSのプログラムに従って、各種処理を制御する。RAM3は、入出力データ及びプログラム実行時のデータ等の一時待避等に使用され、EEPROM4は、不揮発的にデータを保持するとともに書き換え可能にデータを保持する不揮発性データ記憶手段となる。

【0022】端末装置IFDは、例えばICカード専用のリーダライタであり、ホスト装置HSTは、端末装置IFDにおける動作の制御等を行うものである。また、通信手段I/Oは、ICカードICCと端末IFDとの間で、コマンドやデータを送受信するためのものである。

【0023】B：実施形態の動作

次に、上記構成からなるICカードシステムの動作を説明する。図3は、本ICカードシステムの動作を示すフローチャートである。また、図4は、端末装置IFDにおける暗号化の方法を示す図であり、図5は、ICカードICCにおける復号化の方法を示す図である。まず、CPU1は、ICカードICCに対しての端末装置IFD側から送信された「付加データ」通知コマンドを受け、不揮発性データ記憶手段であるEEPROM4に格納されている「付加データ」の値を端末装置IFD側にレスポンスとして通知する(S31)。なお、「付加データ」通知コマンドは、正当権利者のみが知り得るコマンドである。

【0024】次に、この「付加データ」を受信した端末装置IFD側は、図4に示すように、ICカードにコマンドを発行するために、コマンドのAPDU (Application Protocol Data Unit) 部の最終バイトに当該「付加データNn」を付加し、このデータを秘密鍵によって暗号化して、コマンドとしてICカードに送信する(S32)。CPU1は、図5に示すように、受信したコマンドデータを秘密鍵によって複合化し(S33)、平文の

7
コマンドデータと最終データに付加された「付加データ Nn」とを取り出す (S34)。CPU1は、この取り出した「付加データ Nn」とEEPROM4に格納されている「付加データ」とを比較し (S35)、同一であれば正当権原者からのコマンドであると判断する。

【0025】ここで、CPU1は、正当権原者からのコマンドと判断した場合は、その比較した「付加データ」に1を加算して新しい「付加データ」とし、この新しい「付加データ」をEEPROM4に格納する (S36)。そして、復号化処理によって得られた当該コマンド

10
を実行する処理を行い (S37)、その処理結果をレスポンスデータとして端末装置IFD側に送信する (S38)。
【0026】また、ステップ35において、正当権原者であると判断できなかった場合は、CPU1は、その旨をレスポンスデータとして端末装置IFD側に通知する。このように、CPU1は、EEPROM4に格納されている付加データに対して、端末装置IFD側から一つの命令データを受信する毎に、1を加算する。そして、当該加算後の付加データを新しい「付加データ」として当該命令データに付加する。さらに、CPU1は、付加データが付加された命令データを特定の秘密鍵によって暗号化して通信手段で送受信されるデータとする。

【0027】これらにより、ICカードICCは、不正アクセス者がICカードICCの通信手段に侵入し、正当アクセス者が事前に送信した命令データを当該不正アクセス者が複製して正当な読み出し命令をICカードに対し送信した時でも、この時はすでに付加データを変更しているため、当該不正アクセス者に対して返信データを返信してしまうことを防止することができる。

【0028】C：変形例

本変形例は、本発明の第2の実施形態であり、図1に示す第1実施形態のICカードシステムと同じ構成を有するとともに、以下に述べる機能をも有するものである。図6は、本実施形態のICカードシステムの動作を示すフローチャートである。また、図7は、端末装置IFDにおける暗号化の方法を示す図であり、図8はICカードICCにおける復号化の方法を示す図である。

【0029】まず、CPU1は、ICカードICCに対しての端末装置IFD側から送信された「付加データ」通知コマンドを受け、不揮発性データ記憶手段であるEEPROM4に格納されている「付加データ」の値を端末装置IFD側にレスポンスとして通知する (S61)。次に、この「付加データ」を知り得た端末装置IFD側は、ICカードにコマンドを発行するために、図7に示すように、コマンドのAPDU部の最終バイトに当該「付加データ Nn」を付加し、このデータを秘密鍵によってCBC (Cipher Block Chaining) モードにより暗号化し、認証子生成検査法によるコードであるMAC (Message Authentication Cord) を生成し、この M

ACに平文のコマンドを付加してICカードに送信する (S62)。

【0030】CPU1は、図8に示すように、EEPROM4に格納されている「付加データ」を受信したコマンドデータのAPDU部に付加し、これを秘密鍵によってCBCモードで暗号化してMAC' を生成する (S63)。そして、CPU1は、受信したコマンドに付加されたMACと自らが生成したMAC' とを比較し (S64)、同一であれば正当権原者からのコマンドであると判断する。

【0031】ここで、CPU1は、正当権原者からのコマンドと判断した場合は、「付加データ」に1を加算して新しい「付加データ」とし、この新しい「付加データ」をEEPROM4に格納する (S65)。そして、CPU1は、受信した当該コマンドを実行する処理を行い (S66)、その処理結果をレスポンスデータとして端末装置IFD側に送信する (S67)。また、ステップ64において、正当権原者であると判断できなかった場合は、CPU1は、その旨をレスポンスデータとして

20
端末装置IFD側に通知する。
【0032】これらにより、ICカードICCは、付加データの値を、所定の命令に対する返答データの一部として端末側に通知するので、端末装置IFD側が他の端末装置に変更された場合でも当該所定の命令を送信する端末装置のみ正当権原者と判断することができる。そして、ICカードICCは、正当権原者がMACの照合を終了して、当該コマンドに対する読み出し及び書き込み権を獲得した後に、不正権原者がICカードICCの通信手段I/Oに侵入し、正当権原者が事前に送信した命令データを当該不正アクセス者が複製して正当な読み出し命令をICカードICCに対し送信した時でも、この時はすでに付加データが変更されているため、当該不正権原者に対して返信データを返信してしまうことを防止することができる。

30
【0033】上記実施形態においては、付加データの値を、所定の命令に対する返答データを用いて端末装置IFD側に通知するが、本発明はこれに限定されるものではなく、付加データの値を、各ICカードICCの属性を示すデータである初期応答データ内に含めることで、当該付加データの値を端末側に通知してもよい。

【0034】また、上記実施形態においては、CPU1は正当権原者からのコマンドと判断した毎に付加データに1を加算しているが、本発明はこれに限定されるものではなく、正当権原者からのコマンドと判断した毎に付加データから所定値を減算又は、加算するものでもよい。

【0035】また、加算又は減算に限らず、例えば、乗算や除算あるいは複雑な数式といった演算方法を用いても良い。このような場合は、コマンドに付された「付加データ」とICカードICCに記憶されている「付加デ

ータ」の数値が、同一または所定の差の範囲であれば、両者は一致するものとしてコマンドを送信した者が正当権原者であると判定するようにしてもよい。要は、「付加データ」が、外部装置から受信したコマンドが正当な受信データであることを認証するための認証データとなればよい。

【 0 0 3 6 】

【発明の効果】以上説明したように、この発明によれば、ＩＣカード内に不揮発的に保持される付加データに対して、一つの命令データを受信する毎に、付加データに所定値を一方的に加算又は減算して新たな付加データとし、この付加データを前記命令データに付加し、この付加データが付加された命令データを暗号化して前記通信手段上で送受信されるデータとするので、同じ内容のコマンドをＩＣカード側にする場合でも、そのコマンドを送る毎に毎回異なるデータが必要となる。これにより、この発明によれば、端末側とＩＣカード側とでコマンド／レスポンスのやりとりをする際に、ＩＣカードのセキュリティの根本である正当性認証が終了した後に、不正権原者が通信回線に不正に割り込み、正当権原者が送信したコマンドと同一のコマンドを送信することによって、不正権原者がＩＣカードとの間でコマンド／レス

ポンスのやりとりをすることを防止できるＩＣカードおよびＩＣカードシステムを提供することができる。

【図面の簡単な説明】

【図 1】 本発明の第 1 実施形態であるＩＣカードシステムの構成を示すブロック図である。

【図 2】 従来のＩＣカードの構成を示すフローチャートである。

【図 3】 本発明の第 1 実施形態であるＩＣカードの動作を示すフローチャートである。

【図 4】 図 3 に示すＩＣカードにおける暗号化の方法を示す説明図である。

【図 5】 図 3 に示すＩＣカードにおける暗号化の方法を示す説明図である。

【図 6】 本発明の第 2 実施形態であるＩＣカードの動作を示すフローチャートである。

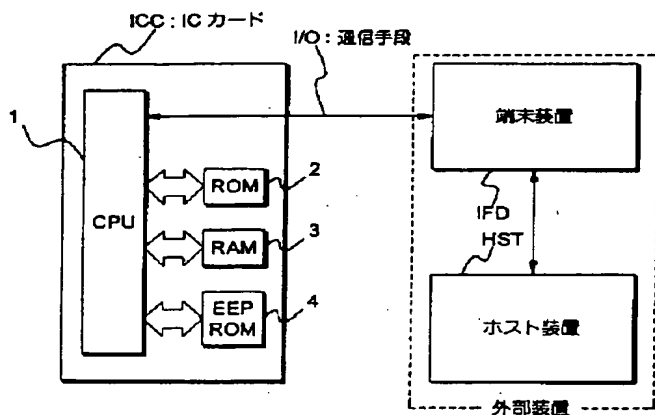
【図 7】 図 5 に示すＩＣカードにおける暗号化の方法を示す説明図である。

【図 8】 図 5 に示すＩＣカードにおける暗号化の方法を示す説明図である。

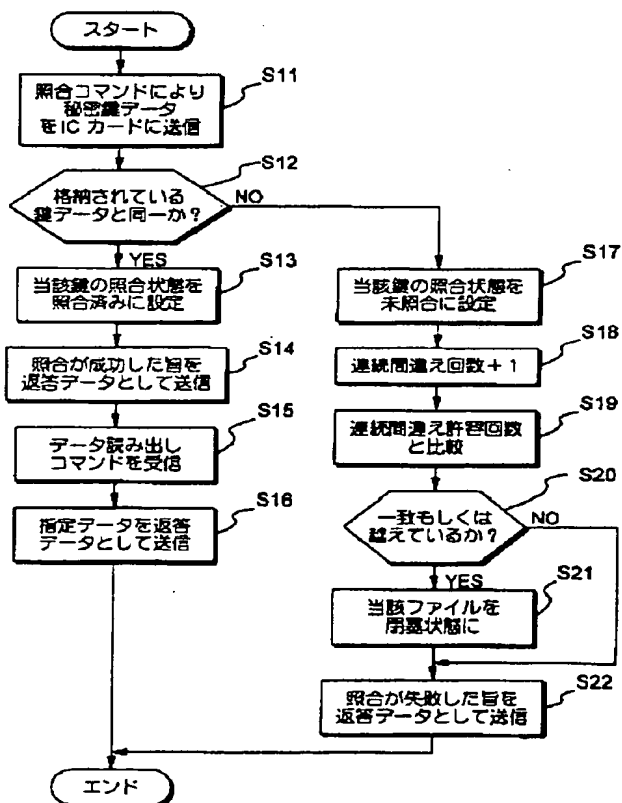
【符号の説明】

1 … CPU、2 … ROM、3 … RAM、4 … EEP ROM

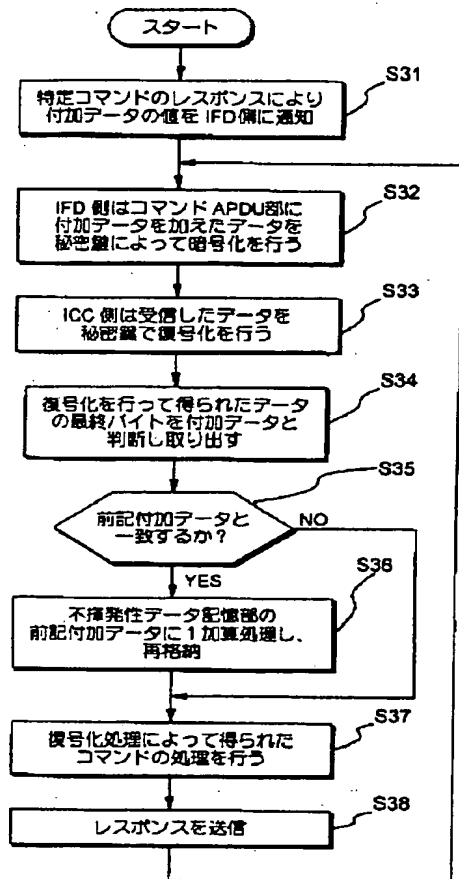
【図 1】



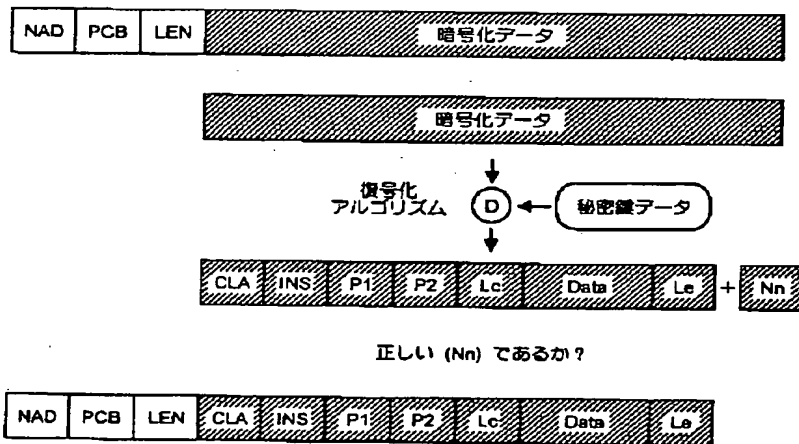
【図 2】



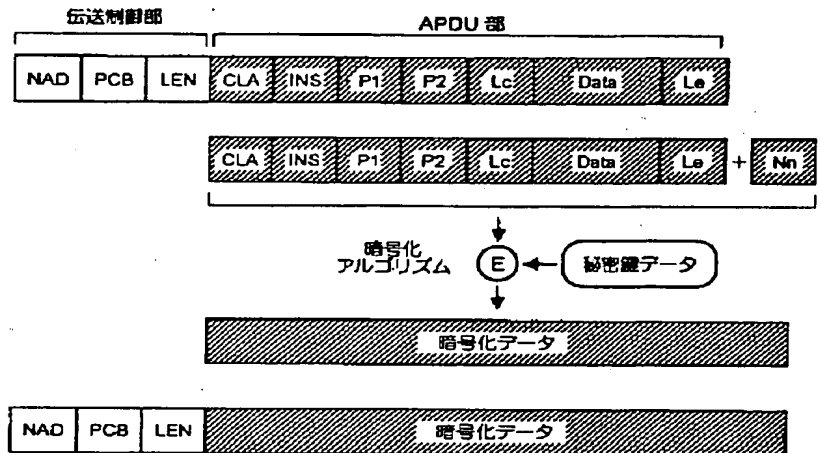
【 図 3 】



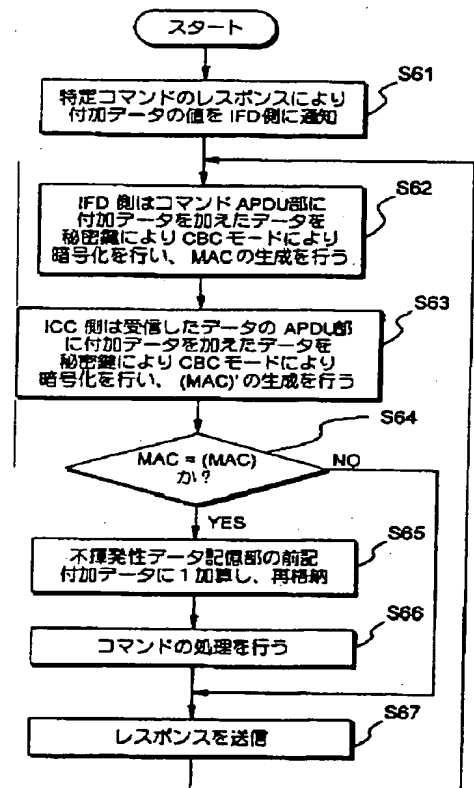
【 図 5 】



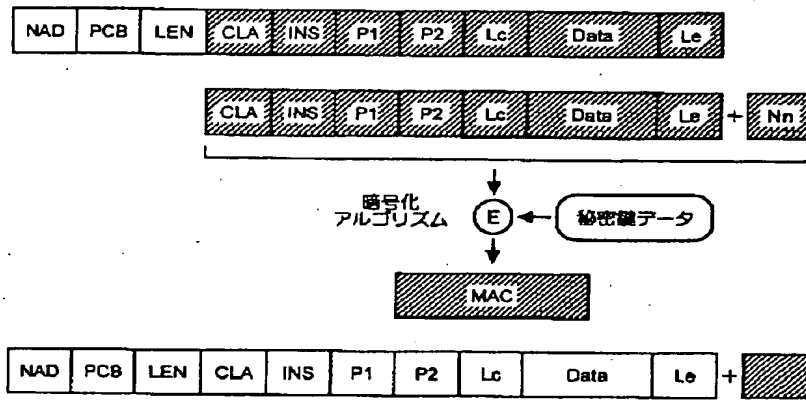
【 図 4 】



【 図 6 】



【 図 7 】



【 図 8 】

